PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-112796
(43)Date of publication of application : 21.04.2000

(51)Int.Cl. G06F 12/00
G06F 12/14
G06F 17/30

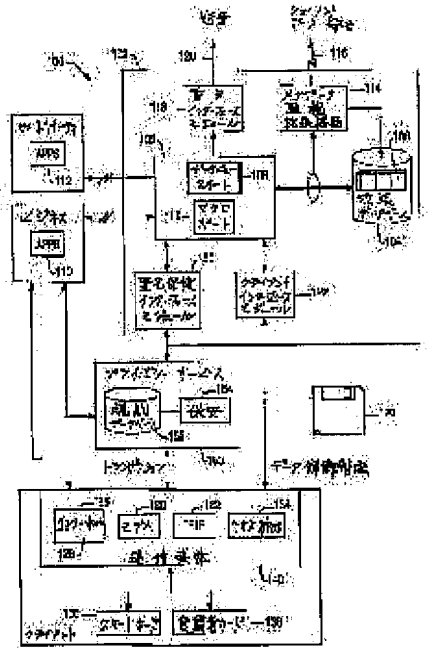
(21)Application number : 11-281593
(22)Date of filing : 01.10.1999

(71)Applicant : NCR INTERNATL INC
(72)Inventor : O FLAHERTY KENNETH W
STELLWAGEN RICHARD G JR
WALTER TODD A
WATTS REID M
RAMSAY DAVID A
ADRIAN W BELDHUISEN
RENDA K OZDEN
PATLARICK B DEMPSTER

(30)Priority
Priority number : 98 165777 ????Priority date : 02.10.1998 ????Priority country : US

(54) METHOD AND SYSTEM FOR MANAGING DATA PRIVACY IN DATABASE MANAGEMENT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To give the whole advantages given by the system while paying attention to privacy by controlling access to data according to a privacy parameter.
SOLUTION: A safety data warehouse 102 includes a suite of privacy meta- data data view 108 that represents the whole data in an expanded database 106, and the data in the database 106 can be seen, processed and changed only through the data view of the suite. Then, a business application 110 and a third party application 112 are only accessible to data that are allowed by the given database view. A client can access, control and manage data collected from the client by using a client interface module 122 communicating with the view 108 and it is accomplished by using a communication medium 140.



LEGAL STATUS
[Date of request for examination] 28.09.2006
[Date of sending the examiner s decision of rejection]
[Kind of final disposal of application other than the examiner s decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

[Date of registration]

[Number of appeal against examiner s decision of rejection]

[Date of requesting appeal against examiner s decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－112796
（P2000－112796A）
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/00	５１２	Ｇ０６Ｆ　12/00	５１２	
	５３７		５３７Ａ	
12/14	３１０	12/14	３１０Ｋ	
17/30		15/40	３２０Ｂ	

審査請求　未請求　請求項の数27　ＯＬ　（全 20 頁）

(21)出願番号　特願平11－281593

(22)出願日　平成11年10月１日(1999.10.1)

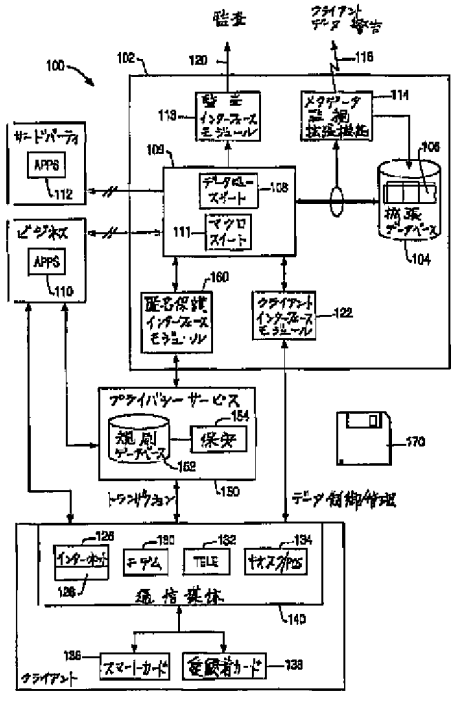
(31)優先権主張番号　０９／１６５７７７
(32)優先日　平成10年10月２日(1998.10.2)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　592089054
エヌシーアール　インターナショナル　インコーポレイテッド
ＮＣＲ　Ｉｎｔｅｒｎａｔｉｏｎａｌ，Ｉｎｃ．
アメリカ合衆国　45479　オハイオ、デイトン　サウス　パターソン　ブールバード　1700
(74)代理人　100098589
弁理士　西山　善章

最終頁に続く

(54)【発明の名称】　データベース管理システムにおけるデータプライバシー管理の方法およびシステム

(57)【要約】
【目的】　データベース管理システムにおけるデータプライバシーを管理する方法、装置および製造方法を提供する。
【構成】　本装置は、複数のデータベース表にデータを格納すると共にその表からデータを取り出すためのデータベース管理システムを含む。このデータベース表内のデータは、データベース表に格納されているプライバシーパラメーターにしたがって制御可能にアクセスすることができる。本装置はまたデータベース管理システムインターフェースを含み、このインターフェースはデータベース管理システムに作動上結合されており、プライバシーパラメーターにしたがってデータベース表内のデータへのアクセスを制御する。本装置はさらに監査モジュールを含む。このモジュールはデータベース管理システムインターフェースと通信できるように結合されており、データベース管理システム内のデータプライバシーパラメーターが有効に適用できるようにする。



【特許請求の範囲】

【請求項１】　複数の行および列にデータを格納する複数のデータベース表にデータを格納し、その表からデータを取り出すデータベース管理システムにして、該データベース表に格納されているプライバシーパラメーターにしたがって該データベース表のデータが制御可能にアクセスできる、データベース管理システムと、
該データベース管理システムに動作上結合されており、該プライバシーパラメーターにしたがって該データベース表内のデータへのアクセスを制御する、データベース管理システムインターフェースと、
を含むことを特徴とする、データウェアハウス化兼管理兼プライバシー制御システム。

【請求項２】　該データベース管理システム内の該データプライバシーパラメーターの適用を有効にするため、該データベース管理システムインターフェースと通信すべく結合された監査モジュールをさらに含むことを特徴とする、請求項１に記載のシステム。

【請求項３】　データソースと該データベース表へアクセスする主体との間の通信を匿名化するため、データソースにより選択的に呼び出すことが可能な信託プロキシサービスをさらに含むことを特徴とする、請求項２に記載のシステム。

【請求項４】　該データベース管理システムインターフェースに動作上結合されており、データソースからデータプライバシープレファレンスデータを受信すると共に該データプライバシープレファレンスデータを該データベース管理システムインターフェースに与える手段を含む、データソースインターフェースモジュールをさらに含むことを特徴とする、請求項２に記載のシステム。

【請求項５】　該データソースインターフェースモジュールがさらに、該データベース管理システムからプライバシーパラメーターを取得すると共に該プライバシーパラメーターを該データソースに与える手段を含むことを特徴とする、請求項４に記載のシステム。

【請求項６】　データソースの固有の同定データおよび通信保安情報を格納しているプライバシーデバイスを受信するためのデータソースサービスモジュールをさらに含むことを特徴とする、請求項２に記載のシステム。

【請求項７】　プライバシーデバイスを受信する該手段がさらにプライバシーデータベースを発行する手段を含むことを特徴とする、請求項６に記載のシステム。

【請求項８】　当該データに対するプライバシーパラメーターを集合的に記述するプライバシーデータを格納するプライバシー制御列が該データベース表に増加されることを特徴とする、請求項２に記載のシステム。

【請求項９】　フィールドを含むプライバシー制御列であってそのフィールドがそのフィールドに関連するデータに適用されるプライバシーパラメーターを格納するようにされたプライバシー制御列が該データベース表に増加されることを特徴とする、請求項８に記載のシステム。

【請求項１０】　該データベース管理システムが、該データベース管理システムから送られるすべてのデータが通過する複数の強制データビューを有するデータビュースイートを含むことを特徴とする、請求項２に記載のシステム。

【請求項１１】　該データベース管理システムが、データリクエストをデータベース照会に翻訳するマクロスイートを含むことを特徴とする、請求項２に記載のシステム。

【請求項１２】　該監査モジュールが、該データベース管理システムインターフェースの現在時点における一貫性を監査することを特徴とする、請求項２に記載のシステム。

【請求項１３】　データベース表内に格納されているデータ対するプライバシーパラメーターの格納と取り出しを行うため該データベース表を拡張するステップにして、該データに関連する複数のデータベース表の列内に集合的に該プライバシーパラメーターが格納されるステップと、
該データソースからプライバシーパラメーターを受信するステップと、
該データに関連する列に該プライバシーパラメーターを格納するステップと、
個人プライバシーパラメーターにしたがってデータベース管理システムインターフェースを介してのみ、該データベース表内のデータへのアクセスをリクエスト主体に与えるステップと、
該データベース表へのアクセスをアクセスログ（access log）内に記録するステップと、
を含むことを特徴とする、データウェアハウス化兼プライバシー制御システム内のデータソースから得られるデータを管理する方法。

【請求項１４】　該アクセスログが、該データへのアクセスを来すＳＱＬステートメントを含むアクセスデータを含むことを特徴とする、請求項１３に記載の方法。

【請求項１５】　該データベース表内のデータへのアクセスを与える該ステップが、
リクエスト主体からデータリクエストを受信するステップと、
該リクエスト主体の身元に基づいて選択されるデータビューを与えるステップにして、該データビューが匿名化データビューおよび適用除外選択データビューを含むデータビュー群から選択されるようにされたステップと、
を含むことを特徴とする請求項１３に記載の方法。

【請求項１６】　該データベース表内のデータへのアクセスを与える該ステップが、
リクエスト主体からデータリクエストを受信するステップと、

該リクエスト主体の身元に基づいて選択されるマクロを与えるステップと、を含むことを特徴とする請求項１３に記載の方法。

【請求項１７】　該個人的プライバシーパラメーターが適用除外選択デフォルト値を含むことを特徴とする、請求項１３に記載の方法。

【請求項１８】　信託プロキシサービス内のデータソースから、トランザクション主体の身元データを含むプロキシサービスリクエストを受信するステップと、
該データソースと該トランザクション主体との間の通信を匿名化するステップと、をさらに含むことを特徴とする請求項１３に記載の方法。

【請求項１９】　該データソースからアクセスリクエストメッセージを受信するステップと、
該データソースの個人プライバシーパラメーターへのアクセスを与えると共に該データソースの個人プライバシーパラメーターへの変更を許す特権データビューを該データソースに与えるステップと、をさらに含むことを特徴とする請求項１３に記載の方法。

【請求項２０】　コンピューターによる読み取りが可能であり、該コンピューターにより実行可能な一つ以上の命令を実行してデータウェアハウス化兼プライバシー制御システム内のデータを管理する方法ステップを行うためのプログラム格納デバイスであって、該方法ステップが、
データベース表内に格納されているデータ対するプライバシーパラメーターの格納と取り出しを行うため該データベース表を拡張するステップにして、該データに関連する複数のデータベース表の列内に集合的に該プライバシーパラメーターが格納されるステップと、
該データソースからプライバシーパラメーターを受信するステップと、
該データベース表の列に該個人プライバシーパラメーターを格納するステップと、
個人プライバシーパラメーターにしたがってデータベース管理システムインターフェースを介してのみ、該データベース表内のデータへのアクセスをリクエスト主体に与えるステップと、
該データベース表へのアクセスをアクセスログ（access log）内に記録するステップと、を含む方法であることを特徴とする、プログラム格納装置。

【請求項２１】　前記プログラム格納デバイスにおいて、該アクセスログが該データへのアクセスを来すＳＱＬステートメントを含むことを特徴とする、請求項２０に記載のプログラム格納装置。

【請求項２２】該データベース内のデータへのアクセスを与える該方法ステップが、
リクエスト主体からデータリクエストを受信するステップと、
該リクエスト主体の身元に基づいて選択されるデータビューを与えるステップにして、該データビューが匿名化データビューおよび適用除外選択データビューを含むデータビュー群から選択されるようにされたステップと、を含む方法であることを特徴とする、請求項２０に記載のプログラム格納装置。

【請求項２３】　該データベース内のデータへのアクセスを与える該方法ステップが、
リクエスト主体からデータリクエストを受信するステップと、
該リクエスト主体の身元に基づいて選択されるマクロを与えるステップと、を含む方法であることを特徴とする、請求項２０に記載のプログラム格納装置。

【請求項２４】　該個人的プライバシーパラメーターが適用除外選択デフォルト値を含むことを特徴とする、請求項２０に記載のプログラム格納装置。

【請求項２５】　該方法ステップが、
信託プロキシサービス内のデータソースから、トランザクション主体の身元データを含むプロキシサービスリクエストを受信するステップと、
該データソースと該トランザクション主体との間の通信を匿名化するステップと、を含む方法であることを特徴とする、請求項２０に記載のプログラム格納装置。

【請求項２６】　該方法ステップが、
該データソースからアクセスリクエストメッセージを受信するステップと、
該データソースの個人プライバシーパラメーターへのアクセスを与えると共に該データソースの個人プライバシーパラメーターへの変更を許す特権データビューを該データソースに与えるステップと、を含む方法であることを特徴とする、請求項２０に記載のプログラム格納装置。

【請求項２７】　複数の行および列にデータを格納する複数のデータベース表にデータを格納しその表からデータを取り出すためのデータベース管理システムにして、
該データベースに格納されているプライバシーパラメーターにしたがって該データベース表内のデータが制御可能にアクセスできる、データベース管理システムと、
プライバシーデータを登録すると共にデータ、ユーザーおよびデータの使用のすべてを統括し、かつ該プライバシーパラメーターにしたがって該データベース表内のデータへのアクセスを制御する、プライバシーメタデータシステムと、を含むことを特徴とする、データウェアハウス化兼管理兼プライバシー制御システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はデータのウェアハウス（倉庫）化および解析の方法およびシステムに関し、特にデータベース管理システムにプライバシー制限を課する方法およびシステムに関する。

【０００２】

【従来の技術】データベース管理システムはデータを収集、流布、および解析するのに使われる。このような大規模統合データベース管理システムは大量のデータを格納し、取出し、解析するための、効率的で一貫したかつ安全にデータのウェアハウス化を行う能力を提供する。大量の情報を収集、解析および管理を行うこの能力は、今日のビジネス界においてほぼ必須のものとなっている。

【０００３】これらのデータウェアハウスに格納される情報は種々のソースから到来しうる。一つの重要なデータウェアハウス化アプリケーションはビジネス機関と消費者との間の商取引の過程で収集される情報の収集および解析を行う。例えば、ある個人が小売店である物品を購入するためにクレジットカードを使用すると、顧客の同定、購入物品、購入額その他の関連情報が収集される。従来、このような情報は当該取引を完了すべきか否かを決定するため、および製品在庫を制御するために小売業者が使用している。そのようなデータはまた、現在の購入傾向および地域的購入傾向を決定するのにも使用することができる。

【０００４】他の産業界でも個人データの使用が同様に行われている。例えば、銀行業務においては顧客の購買パターンはそのクレジットカード取引プロファイルまたは当座／預金口座の活動を解析することにより予測することができ、またある種のプロファイルをもつ顧客達は抵当や個人的退職者口座のような新規サービスを求める潜在的顧客として同定することができる。さらに、通信産業界では、通話記録から消費者通話パターンを解析することができ、ある種のプロファイルをもつ個人を２本目の電話線あるいはコールウェイテシングのような更なるサービスの販売の対象として特定することができる。

【０００５】さらに、データウェアハウス保有者は、普通、取引データを豊富にするためのデータをサードパーティー（第三者）から購入する。この豊富化のプロセスは家族構成員の会員権、収入、雇用主、その他の個人データなどの人口統計データを豊かにする。

【０００６】そのような取引期間中に収集されたデータは他の用途にも有用である。例えばある特定の取引に関する情報は当該消費者についての個人情報（年齢、職業、住居地、収入等）に相関づけて統計的情報を発生させることができる。ある場合にはこの個人情報は大まかに、当該消費者の身元（identification）を表す情報とそうでない情報との二つのグループに分類することができる。消費者の身元を表さない情報は有用である。なぜならばそれが類似の個人的特徴をもつ消費者達の購入傾向に関する情報を得るのに使用することができるからである。消費者の身元を表す個人情報はより絞り込んだ個人的市場戦略に使用することができる。その場合、各個人消費者の購入習慣が解析されて別の市場の候補者あるいはある好みに合わせて手直しした市場の候補者が同定される。

【０００７】個人データの収集が増大している別の例は、最近の「会員制」カードあるいは「愛顧者」カードの繁栄に現れている。これらのカードはある種の製品について顧客に割引価格を提供する。しかし顧客がそのカードを購入に使用する度に、顧客の購入習慣に関する情報が収集される。オンライン環境あるいはスマートカード、電話カードおよび借入カードすなわちクレジットカードでも同じ情報が得られる。

【０００８】そのようなデータの収集および解析が大きな大衆的利益になりうるものの、それは残念ながらかなり悪用の対象ともなりうる。愛顧者プログラムの場合、かかる悪用の可能性が、本来は協力的な多数の消費者が会員賞やその他のプログラムを得るのに参加することを阻害しかねない。またかかる悪用はキャッシュカードのような将来的技術を使用することを拒ませ、現金および小切手のようなより保守的な支払方法を継続することを助長する。実際、プライバシーに関する公衆の心配が、ウェブ商業が爆発的成長するとの期待を遅らせている要因であると信ぜられる。

【０００９】これらすべての理由から、通常の制約と同様、個人情報がデータウェアハウスに格納されるとき、データを制御する者達はそのような悪用からデータを保護することを要求される。このコンピューター時代にあって、データが益々収集されるにつれて個人に関するデータの使用上、個々人の権利が益々重要になっている。

【００１０】

【発明が解決しようとする課題】本発明の課題は、消費者のプライバシーに対する関心に注意を払いつつ、完備したデータウェアハウスシステムが与えうるすべての利点を与えるシステムおよび方法を提供することである。

【００１１】

【課題を解決するための手段】本発明はその第一の局面から見ると、データウェアハウス化兼管理兼プライバシー制御を行うシステム（data warehousing, management, and privacy control system）であって、複数の行および列にデータを格納する複数のデータベース表にデータを格納し、またその表からデータを取り出すデータベース管理システムにして、該データベース表に格納されているプライバシーパラメーターにしたがって該データベース表のデータが制御可能にアクセスできる、データベース管理システム（database management system）と、該データベース管理システムに動作上結合されており、該プライバシーパラメーターにしたがって該データベース表内のデータへのアクセスを制御する、データベース管理システムインターフェースとを含むことを特徴とするデータウェアハウス化兼管理兼プライバシー制御システムに存する。

【００１２】第二の局面から見ると、本発明はデータウェアハウス化兼プライバシー制御システム内のデータソ

ースから得られるデータを管理する方法であって、データベース表内に格納されているデータ対するプライバシーパラメーターの格納と取り出しを行うため該データベース表を拡張するステップにして、該データに関連する複数のデータベース表の列内に集合的に該プライバシーパラメーターが格納されるステップと、該データソースからプライバシーパラメーターを受信するステップと、該データに関連する列に該プライバシーパラメーターを格納するステップと、個人プライバシーパラメーターにしたがってデータベース管理システムインターフェースを介してのみ、該データベース表内のデータへのアクセスをリクエスト主体に与えるステップと、該データベース表へのアクセスをアクセスログ（access log）内に記録するステップとを含むことを特徴とする方法に存する。

【００１３】別の局面から見ると、本発明はコンピューターで読むことができるプログラム格納デバイスであって、該コンピューターにより実行可能な一つ以上の命令を具備しておりデータウェアハウス化兼プライバシー制御システム内のデータを管理するための方法ステップを行うことができ、該方法ステップが、データベース表内に格納されているデータに対するプライバシーパラメーターの格納と取り出しを行うため該データベース表を拡張するステップにして、該プライバシーパラメーターが該データに関連する複数のデータベース表の列内に集合的に格納される、ステップと、該データソースからプライバシーパラメーターを受信するステップと、該データに関連する列に該プライバシーパラメーターを格納するステップと、個人プライバシーパラメーターにしたがってデータベース管理システムインターフェースを介してのみ、リクエスト主体に対してリクエスト全体に対するデータベース表内データへのアクセスを与えるステップと、該データベース表へのアクセスをアクセスログ内に記録するステップとを含む方法であることを特徴とするプログラム格納デバイスに存する。

【００１４】さらに別の局面から見ると、本発明はデータウェアハウス化兼管理兼プライバシー制御システムであって、複数の行および列にデータを格納する複数のデータベース表にデータを格納し、その表からデータを取り出すためのデータベース管理システムにして、該データベースに格納されているプライバシーパラメーターにしたがって該データベース表内のデータが制御可能にアクセスできる、データベース管理システムと、プライバシーデータを登録すると共にすべてのデータ、ユーザーおよびデータの使用を統括し（administering）、かつ該プライバシーパラメーターにしたがって該データベース表内のデータへのアクセスを制御する、プライバシーメタデータシステムとを含むことを特徴とするデータウェアハウス化兼管理兼プライバシー制御システムに存する。

【００１５】

【実施例】添付の図面のみを参照しつつ実施例を通して本発明を以下に説明する。

【００１６】図１はデータウェアハウス化システム１００の概観を表すシステムブロック図である。本システムは、中に一つ以上の拡張データベース（extended databases）１０６を格納するデータベース管理システム（database management system）１０４をもつ、保安データウェアハウス（secure data warehouse）１０２を含む。

【００１７】データベースの一つの重要な能力は、仮想的な表（virtual table）を定義し、その定義をデータベース内にユーザーが定義した名称（ユーザー定義名称）と共にメタデータとして保存する能力である。このオペレーションにより形成されるオブジェクトはビュー（view）あるいはデータベースビュー（data view）として認識される。（以下、本発明で使用される特定のデータビューを「データビュー」と呼ぶ。）データビューは仮想的な表であるから、それが必要とされるまではデータベース内のどこにも物理的に顕在化されない。データへのすべてのアクセスは（管理上の目的で行われるデータアクセスは例外として）、データビューを介して達成される。種々のプライバシー規則（privacy rules、プライバシーを保護するための規則）を与えるため、一揃いの複数データビュー（以下、スイート（suite）という）が設けられる。プライバシーデータビューについてのメタデータ（データビュー名称、データビュー列の名称およびデータ型、並びに行を導出する方法を含む）はデータベースメタデータ内に持続的に格納される。しかしビューにより表される実際のデータはその導出された表と関連づけて物理的にどこにも格納されない。その代わり、データ自体が持続的なベース表（basetable）内に格納され、そのビューの行はそのベース表から導出される。データビューは仮想的な表であるが、ベース表に対してオペレーションを実行することができるのとまったく同様に、データビューに対してオペレーションを実行することができる。

【００１８】保安データウェアハウス（secure data warehouse）１０２はさらに、拡張データベース１０６内のすべてのデータを表すプライバシー メタデータ データビュー（privacy metadata dataviews）１０８スイートを含む。データベース１０６内のデータはこのスイートのデータビューを通してのみ、閲覧、処理、変更をすることができる。拡張データベースおよびデータビューの方式および論理モデルをさらに詳しく図２との関連で述べる。

【００１９】拡張データベース１０６内に格納されているデータへの実質上すべてのアクセスはデータビュースイート１０８を介してのみ与えられる。したがって、ビジネスアプリケーション１１０およびサードパーティア

プリケーション１１２は、与えられたデータベースビューにより許可されるデータのみにアクセスできる。一実施例では、消費者のプライバシープレファランス（preferences、好ましいものとして選択された事項）を無効にしうる方策が与えられる。しかし、そのような環境では、無効の原因がデータベースに記載され、それを監査モジュール（audit module）１１８が取り出すことができる。したがって無効化が内密に起きることはできない。さらに、無効化はプライバシーメタデータ監視拡張機能（privacy metadata monitoring extensions、以下ＰＭＤＳ拡張機能または単にメタデータ監視拡張機能という）１１４によって監視することができ、無効化が起きるときは消費者に警告を与える。

【００２０】データベースへのアクセスは、プライバシーデータビュースイート１０８により次の三つの目的の場合に制限して与えられる：（１）個人データを匿名にするを可能にするためのプライバシー規則を用意すること、（２）適用除外選択をした列へのアクセスを制限すること（これはすべての個人データ、別の範疇の個人データおよび個人データ列に適用しうる）、および（３）顧客の適用除外選択に基づいて適用除外選択のために全行（顧客レコード）を削除すること（これによって、取り扱い中の顧客に対して何らかの有効な適用除外選択フラッグが設定されている行を削除し、したがってこれによっていかなる直接販売もサードパーティへの公開も阻止する）。

【００２１】データビュー１０８と通信するクライアントインターフェースモジュール１２２を使用して、クライアント１２４はクライアント１２４から収集されたデータにアクセスし、制御し、管理することができる。このデータの制御および管理は、（適当なブラウザプラグイン１２８、モデム１３０、音声による電話通信機１３２あるいはキオスク１３４、ＰＯＳにあるその他のデバイスを介する）インターネット１２６を含む広範囲の通信媒体１４０を使用して、達成することができる。そのような通信を助けるため、キオスクやＰＯＳ（販売点）にあるその他のデバイスはスマートカード１３６あるいは愛顧者カード１３８を発行することができる。キオスク／ＰＯＳ装置１３４はプライバシープレファレンスに関する消費者入力を受信し、これらのプレファレンス値に関する情報を格納したスマートカード１３６あるいは愛顧者カード１３８を発行することができる。同様にして、キオスク／ＰＯＳ１３４、スマートカード１３６、あるいは愛顧者カード１３８を使用して、消費者は必要に応じてプレファレンス値を更新し、あるいは変更することができる。愛顧者カード１３８が単純な読取り専用装置（キー リングに装着されたバーコード装置等）である場合は、キオスク１３４は必要に応じて情報を更新した取り替えカードを発行することができる。愛顧者カード１３８あるいはスマートカード１３６を使用する取引は選択的に暗号化し、匿名にすることができる。いずれのカードも選択した保安規則を与えるべく、直接にあるいはプラグインを介してサーバと対話することができる。

【００２２】このインターフェースを介して消費者はデータシェアリング（data sharing）および保持（retention）のプレファレンスを指定することができる。これらのプレファレンスにはデータ保持プレファレンスおよびデータシェアリングプレファレンスが含まれる。これらのプレファレンスによって、消費者はいついかなる状況の下で個人情報を保持し、または共有しあるいは他人に販売しうるかを指定することができる。例えば、当該消費者はそのようなデータを愛顧者カードプログラムの一部として保持することができ、あるいはそのデータの使用を特定の使用に限定することができる。さらに、消費者はいかなる状況の下でそのデータが即時販売され、統計的解析の目的に使用され、あるいはサードパーティの選択的マーケティングプログラムの目的に使用されうるかを指定できる。

【００２３】データデータウェアハウス化システム１００はまた、プライバシーサービス１５０を介してクライアントと保安データウェアハウス１０２との間の匿名通信を可能にする。ユーザーが匿名の取引を望むときは取引はプライバシーサービス１５０へ送信される。プライバシーサービス１５０はプライバシー規則データベース１５２および他の保安情報１５４にアクセスし、プライバシー規則および保安情報を使用して消費者の身元を決定できるすべての情報を除去（浄化）する。浄化された取引情報は次いで保安データウェアハウス内の匿名保護インターフェースモジュール１６０へ回送される。保安データウェアハウス１０２との通信はプロキシユーザー同定手順を使用する。この同定はプライバシーサービス１５０により消費者の使用者名または他の同定情報から生成される。もしも顧客が匿名取引を必要としないなら、取引は、拡張データベース内に取引情報を格納できる小売業者に直接に提供される。

【００２４】データビュースイート１０８は単独に拡張データベース内のデータへのアクセスを与えるので、データビュースイート１０８もまた保安データウェアハウス１０２の保安を監査するための便利かつ合理的手段を与える。

【００２５】保安データウェアハウス１０２もまたメタデータ監視拡張機能１１４を含む。このメタデータ監視拡張機能１１４によって顧客は個人データの使用を監視するための規則を発生させることができ、またメタデータ定義の変更が生じたときは警告１１６または取り消しを送信することができる。顧客の個人情報が拡張データベース１０６から読み取られるとき、または拡張データベース１０６に書込みがなされるとき、拡張データベース１０６に格納されている適用除外選択デリミタ（opt-

out delimiters）が変更されとき、あるいは表またはデータビューがアクセスされるときに、消費者はメタデータ監視拡張機能１１４を制御して警告を発生させることができる。この代わりに、顧客が後でアクセスできるよう、発生した警告を記録しておくことができる。

【００２６】メタデータ監視拡張機能１１４はまたデータソース情報を記録するので、顧客は保安データウェアハウス１０２に格納されているデータのソースを決定することができる。データソースは顧客であるかも知れないし、あるいはサードパーティを媒介とするソースであるかも知れない。本発明のこの特徴は、顧客が誤った情報を訂正したいときのみならず、当該誤りが同じデータベースもしくは他のデータベースで繰り返されることがないよう、誤った情報ソースを特定したいとき、特に有用である。

【００２７】またデータのソースを直接に表データから確かめることができるよう、ソースデータはデータ表の各列にあるいは一組の列に格納することもできる。本実施例では、メタデータ内に情報ソースの情報をすべての顧客に対して複製することをしなくても各顧客が異なった情報ソースをもつことができるよう、ソースを同定するデータを一般化することができる。

【００２８】同様にしてメタデータ監視拡張機能１１４も、データターゲット情報を記録するので、顧客は誰が彼らの個人情報の受信者であるかを決定することができる。この特徴もまた顧客の個人情報に関して公開活動を監視する上で有用であるのみならず、複製された誤りを訂正する上で、有用である。

【００２９】メタデータ監視拡張機能１１４はまた、プライバシーデータビュースイート１０８への変更のみならず拡張データベース１０６からの読み取りおよびそれへの書き込みを追跡することにより、監視機能のサポートに使用することができる。

【００３０】本発明は、プロセッサおよびランダムアクセスメモリ（ＲＡＭ）のようなメモリを含むコンピューターに実現することができる。そのようなコンピューターは普通、ディスプレイと動作上結合しうる。ディスプレイは、ユーザー向けウィンドウのようなイメージをグラフィックユーザーインターフェース上に呈示する。コンピューターはキーボード、マウス装置、プリンタ等の他の装置に結合することができる。もちろん、当業者は上記のコンポーネントの任意の組合せあるいは任意数の異種コンポーネント、周辺機器その他の装置をコンピューターに使用することができることを認識できよう。

【００３１】一般に、コンピューターはメモリ内に格納されているオペレーティングシステム、およびユーザーインターフェースの制御の下に動作する。ユーザーインターフェースは入力およびコマンドを受信すると共にグラフィックユーザーインターフェース（ＧＵＩ）モジュールを介して結果を呈示する。ＧＵＩモジュールは普通、別個のモジュールであるが、ＧＵＩ機能を実行する命令はオペレーティングシステムまたはアプリケーションプログラム内に常駐させ、分布させ、あるいは特別の目的のメモリおよびプロセッサを使って用意することができる。コンピューターはまた、ＣＯＢＯＬ、Ｃ++、ＦＯＲＴＲＡＮその他のプログラム言語で書かれたアプリケーションプログラムがプロセッサで読み取りできるコードに翻訳しうるコンパイラをもつことができる。翻訳完了後、アプリケーションは、コンパイラを使って発生された諸関係式および論理を使用してコンピューターメモリ内に格納されているデータにアクセスし、操作する。

【００３２】本実施例では、オペレーティングシステムをなす諸々の命令、コンピュータープログラムおよびコンパイラはコンピューターが読み取り可能な媒体、すなわちデータ格納装置１７０内に実体的に実現される。この格納装置１７０はジップドライブ、フロッピーディスク、ハードウェアドライブ，ＣＤ－ＲＯＭドライブ、テープドライブ等の一つ以上の固定式もしくは着脱式データ格納装置でよい。さらに、オペレーティングシステムおよびコンピュータープログラムは諸々の命令からなるが、これらの命令は、コンピューターにより読み取られて実行されると本発明を実現およびまたは使用するのに必要な諸ステップをコンピューターに行わせるものである。コンピュータープログラムおよびまたは諸々の命令もメモリおよびまたはデータ通信デバイス内に実体的に実現することができ、それにより本発明に基づくコンピュータープログラム製品あるいは製造物品を作製することができる。上記のとおりであるから、「プログラム格納装置」、「製造物品」および「コンピュータープログラム製品」と言う用語はここではコンピューターにより読み取り可能な任意の装置、あるいは媒体からアクセス可能なコンピュータープログラムを含む。

【００３３】当業者は、本発明の範囲から逸脱することなくこの形態に任意の改変を加えることができることを認識されたい。例えば当業者は上記のコンポーネントの任意の組合せ、あるいは任意数の異なるコンポーネント、周辺機器その他の装置を本発明に使用することができることを認識されたい。

【００３４】論理モデル

図２は保安データウェアハウス１０２およびデータビュースイート１０８の論理モデル例をより詳細に示す図である。拡張データベース１０６は表２０２を含んでおり、この表は次の三つの部分：同定情報部分２０４、個人情報部分２０６、および機密情報部分２０８に分割される。個人情報部分２０６はデータ列２２０、２３２、２４４、および２４６を含み、これらの列は消費者の身元を表す情報を格納する。これらの列には消費者口座番号列２２０、氏名列２３２、住所列２４４、および電話番号列２４６が含まれる。顧客表２０２の同定部分２０

４も一つ以上のデータ制御列２１２を含んでおり、これらの列はプライバシープレファレンスすなわち表中の関連データに対する「適用除外選択」を反映するデータを特定している。ここに例示した実施例では、列２２２-２３０は一つ以上の文字（［Ａ」または［Ｄ」）すなわち当該顧客のデータレコードに対するプライバシープレファレンスを指定するフラッグ（［１」および［０」で表されている）を格納する。ここに開示する実施例ではこれらのプライバシープレファレンスは次の事項に対する「適用除外選択」を含む：（１）直接販売、（２）当該顧客を同定する情報および個人データの公開、（３）匿名による個人データの公開、（４）自動マーケティングの判定を行うための個人データの公開、および（５）機密データの公開と使用。表２０２はまた、グローバルデータ制御列２１０を含む。この列は顧客が最大限のプライバシーを望むことを示すのに使用することができる。

【００３５】ここに例示する実施例では、「ビル　Ｋジョーンズという名前の顧客がグローバルデータ制御列２１０に「０」を選択することにより、ある程度のデータ収集、解析、あるいは流布を許可している。彼はさらに、彼の身元情報と共にあるいは匿名で、彼の消費者情報を直接販売に使用することができること、およびサードパーティに公開できることを示している。彼は自動処理を行うのにデータを使用することを許可しているので、機密データを流布することを許可するであろう。

【００３６】一実施例では前述の論理モデルを実現するのにテラデータ（TERADATA）データベース管理システムが使用される。これを使用することにはいくつかの利点がある。

【００３７】第一に大量のデータを格納し取り扱えるテラデータの能力が多数のいろいろのビューの構築を容易にするとともに、保安データウェアハウス化システム１００が論理データモデルを第三の正規の形態でもしくは正規の形態に近い形で利用することを可能にする。

【００３８】第二に、データビューサブセットまでデータを狭めるための一連の選択としてＳＱＬ照会（SQL queries）を実行するシステムとは異なって、本テラデータデータベース管理システムは適当なベース表から直接に必要な列を選択するＳＱＬを発生すべくデータビューベース（dataview base）の照会を書き直す。他のビューはデータをビューサブセットにまで狭める前に表全体を作成するが、テラデータは適当な列および行を結果表（処理結果をまとめた表）中に選択的に引き抜くＳＱＬを発生する。この方法は、前述の論理モデルを実現するのに特に有利である。

【００３９】第三に前述の論理モデルは一般に複雑な照会および広範なＳＱＬステートメントを含むデータビューを生ずる。テラデータデータベース管理システムは、そのような照会およびＳＱＬステートメントを最適化するのに特に有効である。

【００４０】上に教示したことを使用して、特別な個々のプライバシー条件に合うよう、かつ各データベースアプリケーションを制御するのに必要な条件に合うよう、代わりの定義データ制御列構造を有する代わりの論理モデルを実現することができる。

【００４１】データビュー

データビュースイート１０８には多数のデータビューが用意されている。これらのデータビューには標準ビュー２６０、特権ビュー（priviledged view）２６２、匿名ビュー（anonumizing view）２６４、および適用除外選択ビュー２６５が含まれる。これらのビューはデータ制御列２１２に置かれている値に基づいて顧客表２０２内のデータへの可視度（visibility）を制限する。

【００４２】標準ビュー２６０は、列２２４内のフラッグ（個人情報および同定情報が流布できることを意味する）あるいは列２２６（個人情報が匿名でのみ流布し得ることを示す）のいずれかがアクティブ化されない限り、個人データを呈示しない。したがって、標準ビュー２６０は消費者が適当なフラッグを適当な値に設定しない限り、個人データを選択的にビューから隠す。

【００４３】スケーラブルデータウェアハウス（scaleable data warehouse, SDW）の顧客データベース統括者（customer database adominstrators）は、ルーチンユーザーに対しては個人情報のすべての列が隠されるように、顧客表（顧客に関する個人情報を含む任意の表）中に入るビューを設定する。これにより、すべてのルーチン決定サポート（routine decision support、DSS）アプリケーションおよびウェアハウスデータへの照会アセスを備えたツールを個人情報の閲覧から適用除外することができ、その結果これらのアプリケーションおよびツールのすべてのエンドユーザーも同様に個人情報の閲覧から適用除外される。

【００４４】既存のＳＤＷ顧客に対して混乱が生じることを最小限に留めるため、プライバシーデータにアクセスする既存のすべてのアプリケーション内のベース表に使用されるものと同一の氏名を使用してデータビューが設立され、その氏名に対応するベース表の氏名が他の値に命名し直すことができる。こうして、既存アプリケーションが（ここではデータビュー経由で）私的データへアクセスしようと試みても、その私的データはユーザーがもつ特権に応じてデータビューによりふるい落とされる。このアプローチを使用すれば既存のアプリケーションを改変する必要はまったくない。その代わり、論理データモデルおよびデータベースの方式が改変され、更なる命名規約が導入される。

【００４５】特権ビュー２６２は、データベースの管理およびまたは維持（例えば新規顧客の挿入、前顧客の削除、住所変更など）に必要とされる特権的（クラス「Ａ」の）アプリケーション１１０Ｂに対してのみ、お

よびプライバシー関連機能（顧客について収集された個人情報を顧客に通知すること、個人情報を変更／更新すること、および「適用選択／適用除外選択」制御を適用することなど）の関連機能）を取り扱うアプリケーションに対してのみ、提供される。例えば、顧客プライバシープレファレンスを閲覧し、指定し、変更するのに使われるクライアントインターフェースモジュール１２２は、特権アプリケーションである。特権アプリケーションが特権アプリケーションであると適切に同定されることを確実ならしめると共に、特権ビュー２６２が承認されていない任意の主体によるアクセスを防止するため、適当な保安対策がとられる。

【００４６】ある種のＳＤＷアプリケーション（「クラスＢ」）は顧客の振る舞いの見通しを得るため、例えば顧客の傾向あるいは行動パターンを同定するため、個人データに解析を施すことができる。そのようなアプリケーションは（知的業務者あるいは「パワーアナリスト」と呼ばれる）エンドユーザーが駆動することができる。かかるエンドユーザーとは即興的に照会を行うことができるエンドユーザー、典型的にはカスタム構築したソフトウェアあるいは標準的照会もしくはＯＬＡＰツールを使って、上記のパターンを発見するようなエンドユーザーである。彼らエンドユーザーは発掘ツール（data mining tools）も使用することができる。このツールでは統計的もしくは機械学習アルゴリズム（machine learning algorithms）が当該アナリストと共にパターンを発見し、そのパターンからアナリストが予測モデルを構築する。

【００４７】最も有効な値を導出するため、解析アプリケーションは利用可能なすべての形態の個人情報にアクセスしなければならない。必要とされる個人のプライバシーを尊重すると同時にそのようなアクセスを可能にするため、特別の「匿名化」データビューが使用される。これらデータビューは個人データフィールドへのアクセスを提供するように設計されているが、データ所有者を同定できる情報（例えば氏名、住所、電話番号、社会保障番号、口座番号など）を含むすべてのフィールドを遮蔽するように設計されている。

【００４８】匿名化ビュー２６４は個人情報の閲覧および解析を許すが、列２２４内のフラッグ（当該消費者を同定する情報と個人データの公開を許可するフラッグ）が選択されていない限り、同定情報部分２０４に格納されている情報を閲覧および解析から遮蔽する。このデータは解析アプリケーション１１０Ｃに提供することができる。このアプリケーションはデータ発掘および即興的照会を許容する。消費者が許可するなら、この情報はまたサードパーティアプリケーション１１２にも与えることができる。

【００４９】別のクラスの特権アプリケーション（「クラスＣ」）にはある形態の処置（action）を行うために個人情報を使用するアプリケーション、たとえばマーケティングアプリケーション（郵便もしくは電話による勧誘を行うものなど）が含まれる。これらのマーケティングアプリケーションは各顧客に対して設定された「適用選択／適用除外選択」制御を受け、アクティブ化された「適用除外選択」指標（indicator）をもつすべての記録を除去しあるいは隠す特別のデータビューを介して、顧客情報にアクセスする。したがって、例えばマーケティング勧誘を受信しない選択をした任意の顧客は、マーケティングアプリケーションが生成する任意の接触リストから適用除外される。

【００５０】「適用除外選択」指標はデータビュー経由で顧客表に追加され、あるいは既存の顧客表に接合される新規の列である。（これは論理データモデルに追加される変更である。）一実施例では、各顧客行に対するこの列の値は、初めは「適用除外選択」に設定される（あるいは法律で許可されるなら「適用選択」に設定される）が、クライアントインターフェースモジュール１２２経由で改変することができる。このモジュール１２２はプライバシー制御に関する顧客のリクエストを処理する。

【００５１】多重「適用除外選択」指標は、各顧客レコードに対して設定することができる。最小限、「直接販売」、「身元データのサードパーティへの公開」、「サードパーティへの匿名データの公開」、「自動判定」、および「機密データの使用」に対する５個の適用除外選択が用意される。しかし、さらに詳細な顧客のプレファランスに基づいてさらに詳細に分類した適用除外選択を設計することができよう。例えば、「直接販売」に対する適用除外選択項目は、電話、ダイレクトメール、および電子メールによる接触、および「その他」の処置のための雑類事項に分けることができよう。こうすると８個の別個の適用除外選択が生じる。

【００５２】適用除外選択ビュー２６６は処置アプリケーション１１０Ｄによって自動判定（automated decisions）を行うために情報を利用することは許可する。そのようなアプリケーションはたとえば電話あるいは郵便による勧誘などの処置を行うものである。この情報の閲覧は列２２８内のフラッグにより制御される。列２２８に格納されている値は、この代わりとして十分な値域をもつ一文字を含むことができる。その文字は、当該勧誘が許可されることを定義するに留まらずいかなる種類および範囲の勧誘が許可されるかを指示することを許容できる。

【００５３】（マーケティングや解析等を目的として）サードパーティに個人データを公開しあるいは照会するアプリケーションはクラスＣ（「適用除外選択」）のビューおよびクラスＢ（「匿名」）のビューの両方を受ける。もしも顧客が、サードパーティによる自分のデータの使用を適用除外とする選択をしていると、「適用除外

選択」データビューが適用され、それらの行（レコード）は出力から適用除外される。他の顧客は彼らのデータが匿名であることを条件にサードパーティへの公開を「適用選択」しているかも知れない。そのような場合には顧客データは出力される前に「匿名化」データビューを介して匿名化される。他のすべての場合は顧客は身元が同定できる形式で自分の個人データが公開されることの適用選択をしている。この場合は個人データが身元同定データと共に出力される。

【００５４】適用選択もしくは適用除外選択をするためのさらに細かい分類を用意することができる。種々の許可および保護に関して顧客毎に同意を求め、特定の適用選択もしくは適用除外選択を設定できる。例えば、サードパーティへの公開は、個人の特徴および個人の身元の両方に関連する特定のデータに基づいて行うことができる。顧客は自分の住所および関心事のプロファイルを提供することに同意するが、経済情報および電話番号については同意しないこともあり得る。

【００５５】適用選択／適用除外選択は各顧客のさらに詳細なプロファイルおよび関心事が得られるようにさらに拡張することができる。例えば、適用除外選択（例えば第４節で同定した８個の適用除外選択）のクラスをそれぞれ別個に各範疇の個人データ（例えば人口統計学的データ、プレファレンスデータなど）に適用することができようし、あるいは個人データの各特定データ項目（例えば年齢、性別、ハイキング趣味、好みの靴ブランドなど）にまで適用することができよう。このようにして、顧客はいくつかの関心領域に関連するいくつかの処置を適用除外選択することができ、他の項目を適用選択する（例えばランニングシューズについてダイレクトメールの受信を適用する）ことができる。

【００５６】図３はさらに細かく分類された適用選択および適用除外選択を備えた保安データウェアハウス１０２の、別の論理モデルを示す。この実施例では、各クラスのプライバシープレファレンスが各範疇のデータ（例えば人口統計など）に別個に適用され、あるいは個人データ（例えば年齢、性別、ハイキングの趣味、あるいは好みの靴ブランド）の各特定データ項目にまで適用される。例えば、消費者ビル・Ｋ・ジョーンズはいくつかの目的には彼の氏名へのアクセス許可するが、その他の目的にはアクセス不可とする選択をなしうる。これらの制限は列３０２-３１０の記入事項として適切な組合せのフラッグを入力することにより選択することができる。同様にしてジョーンズ氏の名前の格納およびまたは使用に関してプライバシープレファレンスを指定するのに列３１２-３２０を使用することができる。列３１２-３２０に定義されたプレファレンスは、列３０２-３１０に記述されたものと異なるかも知れないし、同一かも知れない。本発明はまた、さらに詳細な顧客のプレファレンスに基づいて、前述の保安プレファレンス範例（secure preference paradigm）を細密な多重的プレファレンス（multiple fine-grain preferences）へ拡張することを可能にする。例えば、直接販売は電話、ダイレクトメール、電子メール、および「その他」の処置をとりたいキャッチコールに対する別々のプライバシープレファレンスに分解することができよう。さらに、直接販売の範囲を一回の接触だけを許可するように指定することができよう。

【００５７】別の実施例ではデータ暗号を使用することによって、拡張データベース１０６およびデータビュースイート１０８が果たす特徴的な保安およびプライバシー保護がさらに強化される。これは与えられた行のデータを暗号化コードで暗号化することにより、あるいは各データフィールドに固有の暗号化数を与えることにより、行うことができる。その代わりとして、消費者のプライバシープレファレンスを実行することができるようにいろいろの階層的レベルでデータを暗号化することもできる。

【００５８】一実施例では暗号化技術は任意の同定フィールド上で使用されると共に行単位でも選択的に適用される。この技術によれば、顧客が（例えばデータを発掘する目的などで）匿名のままに留まることを可能にする一方、データ暗号化権を有するアプリケーションもしくはデータ請求者に対しては積極的に身元の同定を受け入れることが可能になろう。

【００５９】データビューのオペレーション

本発明のデータビュースイート１０８におけるデータビューは、ベース表の適当な列および行を結果表中に選択的に引き入れるＳＱＬステートメントを発生する。（データをビューサブセットにまで狭める前に表全体を作成する）従来技術と比較して、本技術はデータ請求者にデータを呈示するのために必要な処理を低減する。

【００６０】データベース所有者すなわちＢＢＢ ＯＮＬＩＮＥ、ＴＲＵＳＴＥ、ＰＲＩＣＥ－ＷＡＴＥＲＨＯＵＳＥ，ＴＲＷ、ＤＭＡあるいはＣＰＡ ＷＥＢＴＲＵＳＴ、あるいはＮＣＲのような独立の監査サービスは、定期的にもしくは苦情を受けたときに、安価にデータベースの見直し（review）を行うことができる。これらの見直しでは論理データモデルとデータベースのスキーム、当該システムを使用するアプリケーションとユーザー、およびテラデータアクセスログが調査される。

【００６１】論理データモデルの見直しでは、データビュー構造を調査し、（個人情報へのアクセスを制限している）正規ユーザー用の「標準」ビュー、解析アプリケーション用の「匿名」ビュー、およびその他のアプリケーション用の「適用除外選択」ビューの存在が調査される。

【００６２】これらのアプリケーションの見直しおよびユーザーの見直しは、アプリケーション、ユーザー、およびそれらに付与されているアクセス権を調査する。こ

の見直しは、「クラスA」特権をもつアプリケーション／ユーザーが「個人データ」データビューへのアクセス権をもっていること、「クラスB」解析アプリケーション／ユーザーが「匿名化」データビューへのアクセス権をもっていること、「クラスC」処置アプリケーション／ユーザーが「適用除外選択」ビューへのアクセス権をもっていること、個人データの出力表あるいはファイルを生成するアプリケーションが「適用除外選択」および「匿名化」ビューへのアクセス権をもっていること、並びに他のアプリケーションが「標準」ビューを使用することの確認を行う。

【0063】最後に、テラデータアクセスログあるいは別のデータベース管理システムから得た類似のログが見直される。これは行われたアクセス活動が当該データソースにより規定されているプライバシーパラメーターに適合していることを確証するためである。

【0064】図4は本発明の特徴であるプライバシー監査オペレーションの概観を表す図である。データ請求主体が拡張データベース106内のデータへのアクセスを望むときはいつでも、リクエストはデータベース管理システムインターフェース109に対してなされ、インターフェース109がプライバシーパラメーターにしたがって当該データベース表内のデータへのアクセスを制御する。当該リクエスト主体のステータスに基づいてデータビュースイート108からリクエスト主体に与えられるデータビューを使って、拡張データベース106の表がアクセスされ、そのデータが提供される。同時に、データベースアクセス（アクセスが不成功であるときはその試みられたアクセス）がアクセスログ（access log）402に記録される。アクセスログ402は、アクセスもしくはアクセスの試みの形態、アクセスを生じたリクエストのテキスト（SQL）、アクセスの頻度、リクエストされた処置、リクエスト主体またはアプリケーション名または識別データ、および参照されたオブジェクト（表、データビューおよびまたはマクロ）に関する情報を含む。アクセスログ402により、データビュースイート108内のデータビュー、マクロスイート111内のマクロ、あるいはデータベース106内のベース表へのすべてのアクセスを監査することができる。アクセス特権を付与しまたは呼び出す総ての活動が同様に監査できる。これが可能であるのは、アクセスログ402の内容と表／データビュー／マクロの定義とからプライバシー規則が施行されているかあるいは破られているか決定ができるからである。

【0065】プライバシー監査モジュール118が設けらるのは、プライバシーパラメーターを有効に適用すべくアクセスログ402内のデータについてプライバシー解析を行うためである。プライバシー監査モジュール118はプライバシーに関するすべてのイベント（event）を追跡し、個人データへのアクセスに関する活動を要約し、プライバシー規則のいかなる疑惑ある違反にもフラッグを立てる。プライバシーテストスイート404は、プライバシー規則を「破る」ことを試みてからアクセスログ402を調査してプライバシー規則が適用されたかあるいは破られたかを決定するプログラムその他の手順を含んでいる。プライバシー監査モジュール118はこれを、顧客プライバシープレファレンスが適用されているか否かを独立に評価するサービス監査者またはデータウェアハウスマネージャが使用できるように、手直しできる。

【0066】メタデータサービス

メタデータサービスはプライバシーメタデータサブシステム（privacy metadata subsystem、PMDS）拡張機能114を含む。PMDS拡張機能114は多数のパラメーターを格納し、追跡するとともにこれらのパラメーターを使ってプライバシーが関わる活動を追跡する。追跡されたパラメーターには、（1）システムに現在あるすべてのデータエレメント（データベース、ユーザー、表、ビューおよびマクロを含む）のデータ復号化、（2）システムに対してソースとなった内部エレメントのデータ復号化、（3）システムに対してソースとなった外部エレメントのデータ復号化、（4）システムにとってターゲットとなった内部エレメントのデータ復号化、（5）システムからエキスポートされたデータエレメントのデータ復号化、（6）すべてのユーザー、グループおよびアプリケーション並びに当該データへのそれらのアクセス権のプロファイル、（7）データのアクセス／更新、表／ビュー／マクロの生成、特権の付与／取消し、ユーザープロファイルの変更、およびトリガーに関するイベント記録を含む。

【0067】PMDS拡張機能114はまた、プライバシーに固執するデータコントローラを支配する実行可能なビジネス規則と、テラデータログ（例えば記録の開始／終了）の操作（manipulations）に関するイベントの記録もしくは別のデータベース管理システムにおけるそれと類似の記録に関するイベントの記録とを格納し管理する。

【0068】また、PMDS拡張機能114はプライバシーが関わるメタデータを見直し、管理するための高レベルGUI406をプライバシー統括者に提供する。このGUIは、すべての顧客（消費者またはデータの主体）の情報に対するデータベースとそれらの表／ビューマクロ構造のグラフィック表示、および関連するユーザー／ユーザーグループの特権のグラフィック表示を含む。またGUI406は、プライバシー統括者がGUI406を介して与える定義に基づき、プライバシー規則を設定すると共にその設定の結果、データビュー、マクロ、もしくはアクセス権を発生するパラメーター駆動手段（parameter-driven means）を提供する。またGUI406は、外部監査者が当該サイトのプライバシー保護

策の見直しを行う際に彼を案内する便宜を提供する。

【0069】PMDS拡張機能114はまた、報告を行う便宜的機能を提供する。これは種々のデータベースおよびPMDSログの内容を解析してプライバシー関連の活動に関して報告を行うものである。プライバシー統括者はそのようなプライバシー報告を対話形インターフェースもしくは印刷された報告を介して見直すことができる。独立の監査者はプライバシー統括者と共に、そのような報告の助けを借りて監査を行うことができる。

【0070】またPMDS拡張機能114は、消費者の個人データおよびそれに関連するプライバシー規則へのアクセス、それらの見直し、および訂正を行う消費者をサポートするためのGUIアプリケーション/ユーティリティを別途提供する。またPMDS拡張機能114は、プライバシー関連のイベントに関するさらに詳細な記録をとるための便宜を提供することもできる。

【0071】マクロ

単独であるいはここに記載するデータビューと組み合わせてマクロ111（すなわちデータベース管理システムインターフェースに格納された手順）を使用してデータの制御とデータへのアクセスを記録することができる。データプライバシーパラメーターを適用すべくマクロを使用する場合は、ユーザーは「選択」アクセス権を与えられない。その代わり、ユーザーは、マクロスイート111内のマクロへのアクセス権を与えられる。このマクロは実際のデータアクセスを行うと共に将来の監査を目的としてアクセスログ402内のイベントを記録する。その場合も、これらのマクロは適用除外選択された行および列へのアクセスを制限する前記ビューを通して当該データに対し実行される。そのようなマクロは単一行アクセスを記録するのに特に適している。

【0072】データ辞典

データ辞典408は、システム内のすべての表、データビュー、およびマクロ、システム内のすべてのマクロ、すべてのユーザーおよび彼らの特権（ユーザーが所有しているマクロに関する特権を含む）を含めたデータベーススキーマに関する情報を格納している。

【0073】プロセス

図5は本発明の一実施例を実行するのに使用されるオペレーション例を示す流れ図である。このプロセスはブロック502に示すように、表のデータに関連をもつ一つ以上の列にプライバシープレファレンスを格納し、それを取り出すため、データベース表を拡張することにより始まる。この拡張されたデータベース106は、データ（個人的および非個人的データ）およびプライバシーパラメーターを格納するための論理モデルを形成する。普通、このデータベースは初め、プライバシーを最大に保護すべく選択されたプライバシーパラメーターが多数入れてある（すべてのデータの収集、解析および流布を適用除外する選択がしてある）。事情が許すときは、初めデータベースはより低度の、ときには最小限の、プライバシー保護を選択するプライバシーパラメーターで多くするすることもできる。

【0074】次にブロック504に示すようにデータソースからプライバシーパラメーターを受信することができる。この意味では通常、そのデータソースはデータの究極的なソース（消費者）である。しかし他の実施例では、データソースは、データをどのように使用するか、もしくは共有するかに関する命令を含んだデータを与えらている、媒介者たるサードパーティであり得る。その場合、これらの命令は、これらの命令に基づいてそのデータが使用されもしくは流布されることを保証しなければならない。

【0075】ブロック504に示すオペレーションはクライアントインターフェースモジュール122とコンピューターのようなクライアントの通信装置とを介して達成することができる。かかるコンピューターはインターネットブラウザ128（ブラウザプラグインを備えたものなど）および電話接続線を備えた簡単なモデム130を走らせているものでよい。このオペレーションは、電話132を介して（実際のあるいはコンピューター上に用意された）サービス担当者に話すことにより、またはキオスクもしくは自動現金預け払い機（ATM）134を通して、またはデータソースプレファレンスを受信しそれをクライアントインターフェースモジュール122へ送信できるその他の装置を通して、行うことができる。これらのいずれの場合でも、データソースは個人データを閲覧すること、およびデータソースの必要条件に合致するプライバシーパラメーターを選択することができる。インターネットブラウザ128、モデム130、キオスクもしくはATM134を通してアクセスが与えられる場合は、上記装置に用意されているプライバシーウィザードを使用することにより、本プロセスの過程でユーザーを案内することができる。データソースは、愛顧者プログラムをもらう交換条件としてデータの収集、解析、あるいは流布の活動のいくつかを適用を受ける、との選択ができる。一旦データソースのプライバシーパラメーターが得られると、それらのパラメーターはプライバシーパラメーターの主体のデータに関連する列内に格納される。これはブロック506に示してある。リクエストをしている主体がデータへのアクセスをリクエストすると、データビュースイート108、マクロスイート111、あるいはその両方を経由してデータベース管理システムインターフェース109を通してのみアクセスが与えられる。したがってデータは確実にデータソースの個人プライバシーパラメーターにしたがって与えられる。

【0076】図6は、データベース管理システムインターフェースを通してアクセスを与えるために使用するオペレーション例を示す流れ図である。第一に、ブロック

６０２に示すように、リクエスト中の主体からデータリクエストが受信される。次に照合確認されたリクエスト主体の身元にしたがって選択されたデータビューが与えられる。リクエスト主体はこのデータビューを使用してデータベースにアクセスし、データを得ることができる。一実施例ではデータビューは前もってリクエスト主体に与えられ、リクエスト主体は所望するデータにアクセスするためにのみそれらを使用することができる。もう一つの実施例ではデータビューはデータリクエストに呼応してリクエスト主体に与えられるが、データビューはそのデータリクエスト、当該データに関連したプライバシーパラメーター、およびリクエスト主体の身元にしたがって手直しされる。

【００７７】図７は本発明の一実施例においてプロキシサービスリクエスト（proxy service request）を受信するために使用するオペレーション例を示す流れ図である。この実施例はクライアント（または消費者）に小売業者その他の主体と匿名の取引を行う能力を与える。これはプライバシープロキシサービスを使って達成される。このプライバシープロキシサービスは消費者と小売業者（またはデータベース管理システム）との間の匿名化インタプリタ（anonimizing interpreter）を与える。プロキシサービスリクエストが（将来のデータソースたる）プライバシープロキシサービス１５０内のクライアントから受信され、受容されると（ステップ７０２）、そのクライアントに対するプロキシの識別データが取り出される。もしもそのクライアントに対するプロキシ識別データが存在しないと、将来の使用に供するためのプロキシ識別データが発生され、クライアントに与えられる。これらの取引はインターネットブラウザプラグイン１２８、モデム１３０、あるいはキオスク/ＡＴＭ１３４を通して行うことができる。クライアントは、小売業者ごとに、あるいは個人情報を収集することができる他の主体ごとに、異なる匿名化プロキシ識別データをもつことができる。その場合、クライアントのプロキシ識別データ管理を援助するための手段が与えられる。これはクライアントのスマートカード１３６上にデータの格納と処理を行うこと、愛顧者カード１３８にデータを格納すること、およびまたはキオスク／ＡＴＭあるいは販売点（ＰＯＳ）１３４において追加的処理を行うことにより、達成することができる。

【００７８】図８はデータソースからアクセスリクエストメッセージを受信するために使用するオペレーション例を示す流れ図である。本発明はまた、クライアント（あるいはデータソース）が特権ビュー２６２を使って個人データにアクセスし、データの収集、格納、および流布を制御することを可能にする。第一に、ブロック８０２に示すように、アクセスリクエストメッセージがクライアントから受信される。次にブロック８０４に示すように特権データビュー２６２がクライアントに与えられる。特権データビュー２６２はクライアントの個人プライバシーパラメーターへのアクセスを与えるとともに、クライアントがこれらのプレファレンスを閲覧し、変更することを許す。

【００７９】代わりの実施例

図９は本発明の代わりの実施例を示すブロック図である。この実施例では、二つのデータベースが使用される。その最初のものは匿名化されたデータベース９０８で、これは表９０６の中に格納されているデータに関連した匿名化されたデータとと筆名（pseudonyms）とを格納する。第二のデータベースは、信託データベース（trusted database）９０４で、筆名を顧客認識情報に関連づける表９０２を格納している。この実施例では顧客の氏名は信託データベース９０４に別個に格納されている。このデータベースはこれをデータ管理システムインターフェース１０９が使用して、顧客の身元を筆名に、したがって匿名化されたデータベース９０８内に格納されているデータに、結びつける。信託データベースは個々人のプライバシーパラメーターをも格納している。

【００８０】クライアントの筆名は、愛顧者カード１３８もしくはスマートカード１３６を発行することによって、またはインターネット１２６もしくはクライアントコンピューターとのオンライン通信により、またはその他の手段により、クライアントに提供される。次いで筆名は消費者の取引に対するプロキシとして使用することができる（したがって収集された任意のデータを匿名のままに保持することができる）。顧客の身元同定のためのデータ発掘を防止するため、必要であれば異なる業者また異なる店舗に対して異なる筆名を使用することができる。

【００８１】顧客は非匿名データの収集、使用、あるいは流布を許可するようにデータプライバシープレファレンスを選択することができる。これらのプレファレンスはデータ管理システムインターフェース１０９により適用され、クライアントにより愛顧者カード１３８、スマートカード１３８、インターネット１２６、およびその他の通信／データ格納方法を使用して提供される。一実施例ではインテリジェントソフトウェア エイジェントがデータ発掘機能を実行して顧客の行動パターンを調査すると共に、発掘した結果に基づいてデータプライバシーパラメーターを提案する。

【００８２】別の実施例では、多重レベル保安プライバシーシステムにおいて別個の信託データベース９０４および匿名データベース９０８を使用する。この場合は異なる法制によるプライバシー保護の条件やいろいろの小売りアウトレットに適応し、またはいろいろの個人プレファレンスを許容するため、ここに開示した暗号化の方法、マクロ、データビューおよびまたは別個のデータベース技術を組み合わせる。

【００８３】図１０はプライバシーデータウェアハウス

の別の実施例を示す図である。前述した実施例における と同様、データベース管理システム１０４のデータへのアクセスは、再びデータビュースイート１０８内のデータビューを介して、あるいはマクロスイート１１１内のマクロ２を介して達成される。この実施例ではプライバシーサービス１５０、クライアントインターフェースモジュール１２２、メタデータ監視拡張機能１１４、および監査インターフェース１１８を含むプライバシーメタデータサービスインターフェース１００２もデータベース管理システム１０４への全アクセスの途中に配置される。プライバシーメタデータサービスインターフェース１００２はそれゆえ、データベース管理システム１０４、データビュースイート１０８内のデータビュー、およびマクロスイート１１１内のマクロへのすべてのアクセスを制御することができる。

【００８４】図１１はプライバシーメタデータサービスインターフェースが介在するデータビューの実施例を示す図である。データベース管理システム１０４の顧客ベース表内のデータの可視性およびデータへのアクセスはデータビューおよびマクロ１１１により与えられる。データの中に入って行われる閲覧は図１１に示す共心的四角形で表してある。消費者アクセスマクロもしくは消費者ビューは、その消費者もしくはデータ主体に関するデータを収容する消費者データベース表の単一行へのアクセスをユーザー／消費者に与える。システムアシスタント１１０２がデータベースのインフラストラクチャーの定義と管理維持をサポートする一方、プライバシーアシスタント１１０４がそれらの表、データビュー、マクロ、ユーザープロファイル、ログ、監査レポートをサポートする。前述の場合と同様、ルーチンアプリケーション１１０Ａは標準ビュー２６０を介して、また解析アプリケーション１１０Ｃは匿名ビューを介して、顧客ベース表にアクセスする。この場合、顧客の身元を同定できるデータは隠されており、処置アプリケーション（マーケティング アプリケーション）１１０Ｄは顧客データの全行が省かれる適用除外選択ビューを介してアクセスし、サードパーティ公開アプリケーション１１２に与えられるデータビューは、適用選択をした顧客のみを表すが身元同定データへのアクセスは許可しない。適用除外選択／匿名化データビューは別個に用意したデータビューで与えることができ、あるいは適用除外選択および匿名化の両方を適用するデータビューで与えることができる。

【図面の簡単な説明】

【図１】データウェアハウス化システム実施例のシステムブロック図である。

【図２】プライバシー拡張顧客表およびデータベースビュー内に格納された顧客表の構造例を示すブロック図である。

【図３】データウェアハウス化システムの別の実施例のシステムブロック図である。

【図４】本発明の特徴であるプライバシー監査オペレーションの概略を表すブロック図である。

【図５】本発明の一実施例を実行するために使用されるオペレーション例を示す流れ図である。

【図６】本発明の一実施例におけるデータベース管理システムインターフェースを介してデータへのアクセスを与えるのに使用するオペレーション例を示す流れ図である。

【図７】本発明の一実施例においてプロキシサービスリクエストを受信するために使用するオペレーション例を示す流れ図である。

【図８】データソースからのアクセスリクエストメッセージを受信するために使用するオペレーション例を示す流れ図である。

【図９】別個に設けた信託データベースを備えたプライバシーデータウェアハウスの別の実施例を示す図である。

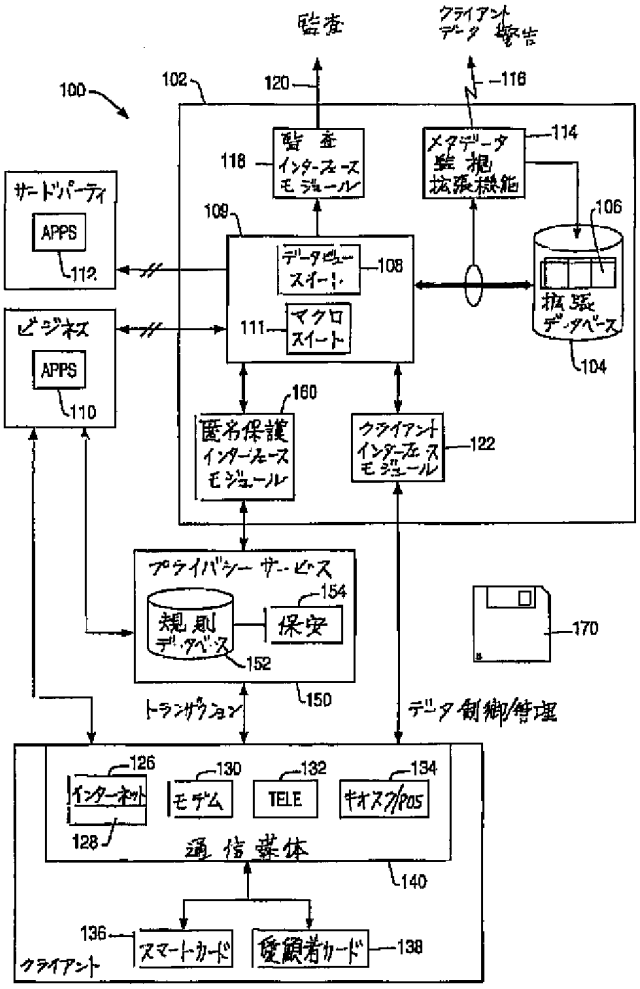
【図１０】すべてのデータアクセスの管理を行いとログをとるべく介在させたプライバシーメタデータ サービスインターフェースを備えた、プライバシーデータウェアハウスの別の実施例を示す図である。

【図１１】プライバシーメタデータ サービスインターフェースが介在するデータビューの実施例を示す図である。

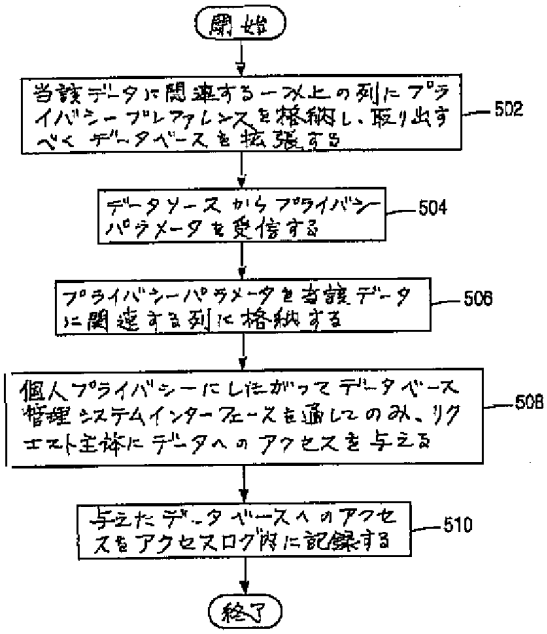
【符号の説明】

１００　データウェアハウス化システム
１０２　保安データウェアハウス（secure data warehouse）
１０４　データベース管理システム（database management system）
１０６　拡張データベース
１２８　ブラウザプラグイン
２０２　顧客表
２０４　同定情報部分
２０６　個人情報部分
２０８　機密情報部分
２１０　グローバルデータ制御列
２１２　データ制御列
９０２　格納表
９０４　信託データベース
１００２　プライバシーメタデータサービスインターフェース
１１０４　プライバシーアシスタント

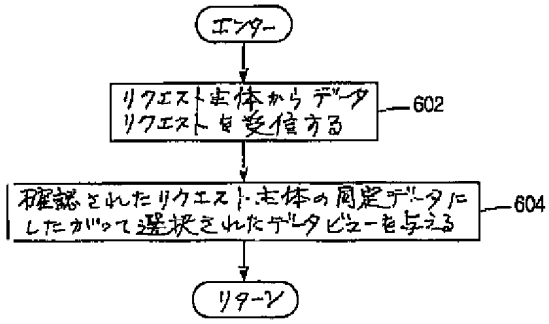
【図1】


監査
クライアントデータ報告
100
102
120
116
118
監査インターフェースモジュール
メタデータ監視拡張機能
114
サードパーティ
APPS
112
109
データビューズ
108
106
111
マクロズ
拡張データベース
ビジネス
APPS
110
104
160
匿名保護インターフェースモジュール
クライアントインターフェースモジュール
122
プライバシーサービス
154
規則データベース
保安
152
150
170
トランザクション
データ制御/管理
126
130
132
134
インターネット
モデム
TELE
ギオス/POS
128
通信媒体
140
136
スマートカード
受領者カード
138
クライアント

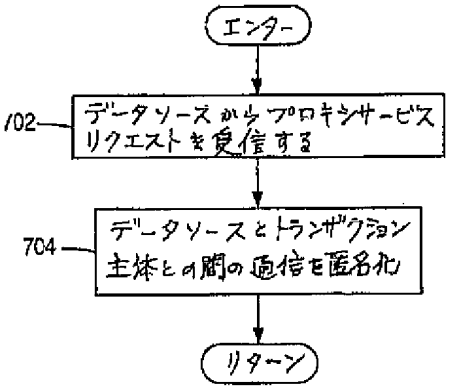
【図5】


開始
当該データに関連する一以上の列にプライバシープレアレンスを格納し、取り出すべくデータベースを拡張する
502
データソースからプライバシーパラメータを受信する
504
プライバシーパラメータを当該データに関連する列に格納する
506
個人プライバシーにしたがってデータベース管理システムインターフェースを通してのみ、リクエスト主体にデータへのアクセスを与える
508
与えたデータベースへのアクセスをアクセスログ内に記録する
510
終了

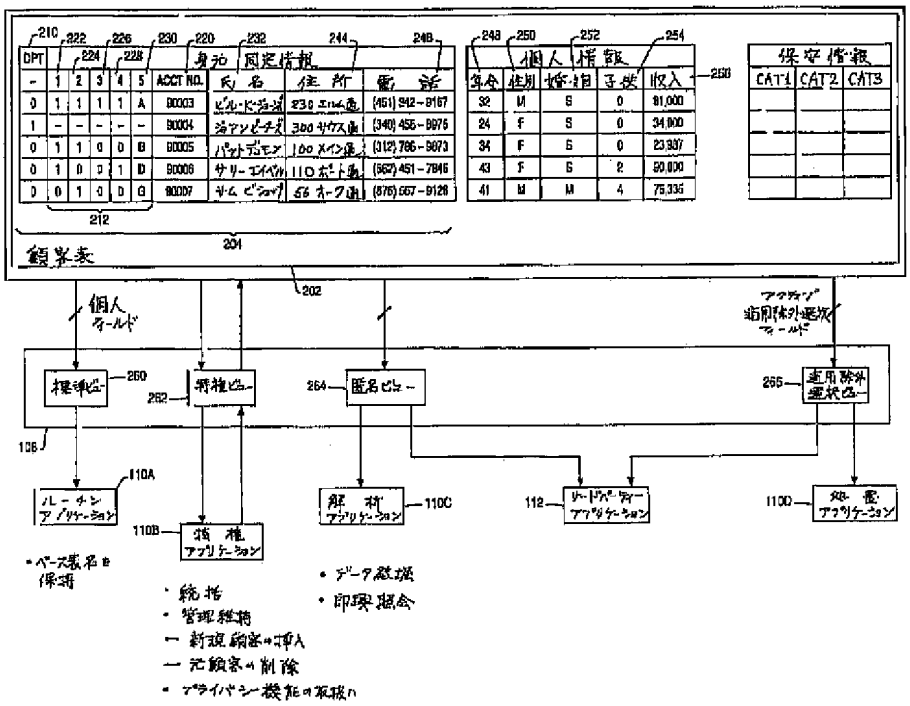
【図6】


エンター
リクエスト主体からデータリクエストを受信する
602
確認されたリクエスト主体の同定データにしたがって選択されたデータビューを与える
604
リターン

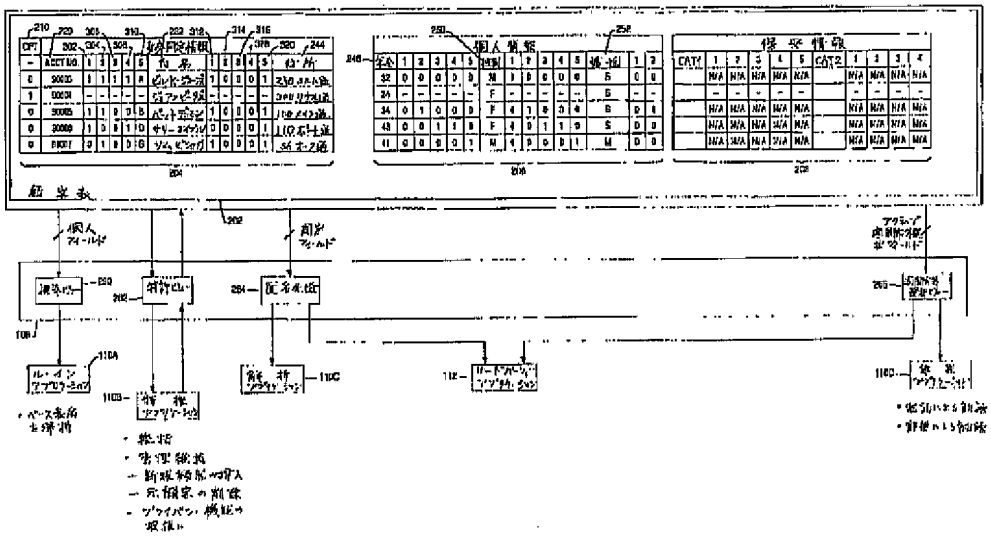
【図7】


エンター
データソースからプロキシサービスリクエストを受信する
702
データソースとトランザクション主体との間の通信を匿名化
704
リターン

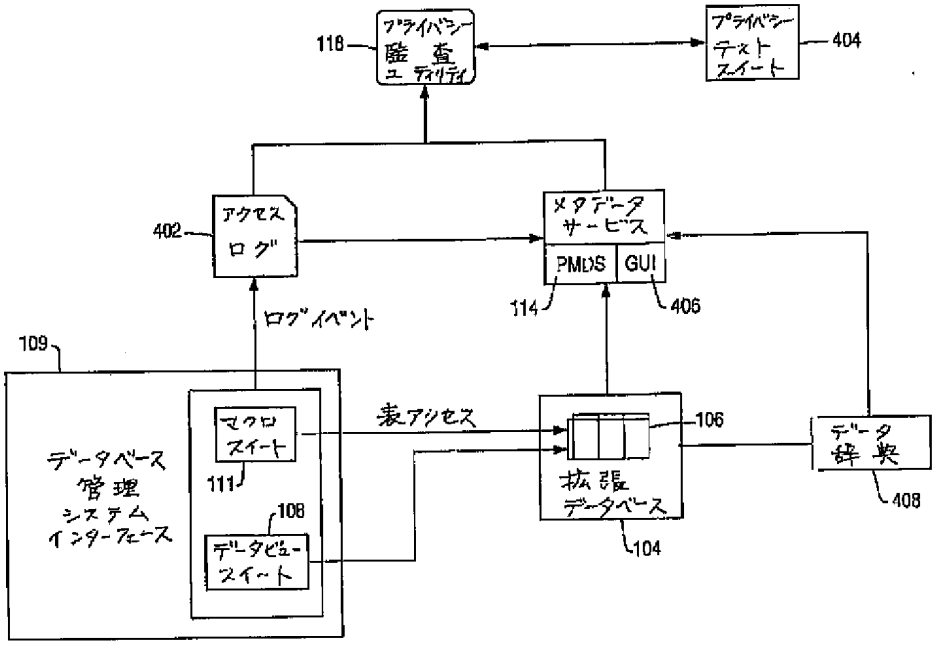
【図2】


顧客表
個人フィールド
属性/非公開属性フィールド
標準ビュー
特権ビュー
匿名ビュー
運用/保守ビュー
ルーチンアプリケーション
特権アプリケーション
解析アプリケーション
リードバック
保守
・統括
・管理維持
・データ登録
・印刷照会

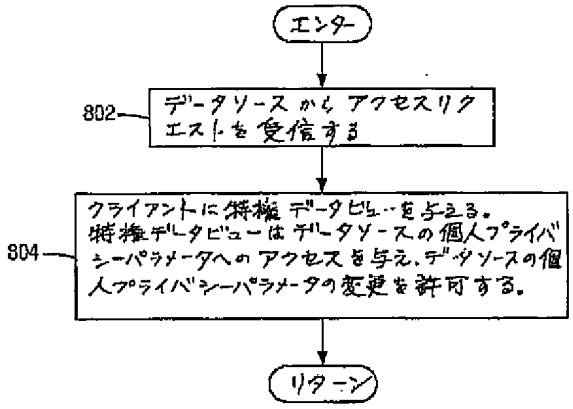
【図3】


顧客表
個人フィールド
属性/非公開属性フィールド
標準ビュー
特権ビュー
匿名ビュー
運用/保守ビュー
ルーチンアプリケーション
特権アプリケーション
解析アプリケーション
リードバック
保守
・統括
・管理維持
・データ登録
・印刷照会

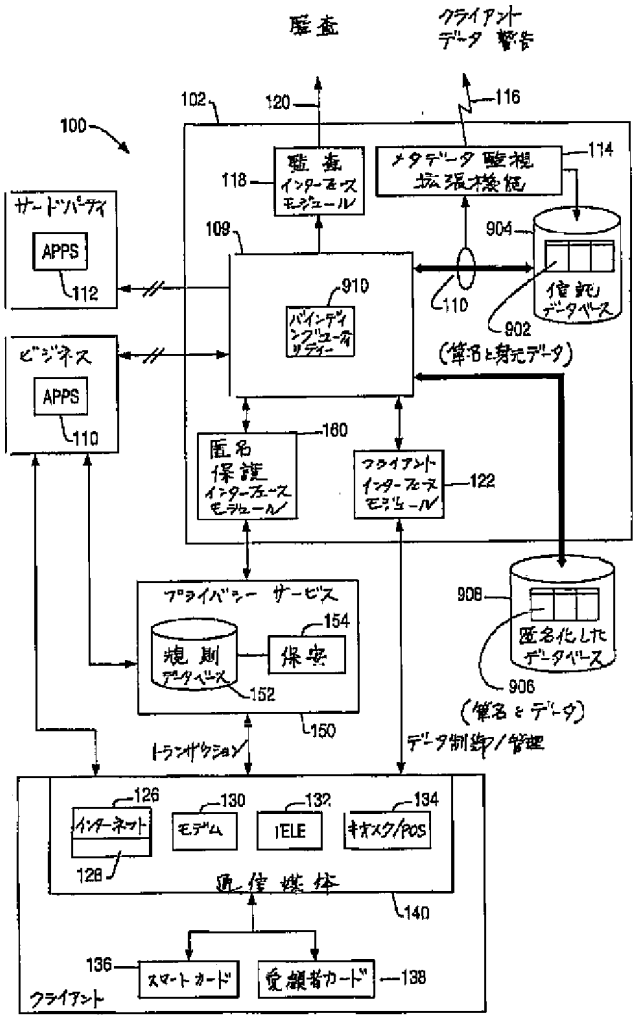
【図4】


118
プライバシー
監査
ユーティリティ
プライバシー
テスト
スイート
404
402
アクセス
ログ
メタデータ
サービス
PMDS
GUI
114
406
ログイベント
109
データベース
管理
システム
インターフェース
マクロ
スイート
111
表アクセス
106
データ
辞典
408
108
データビュー
スイート
拡張
データベース
104

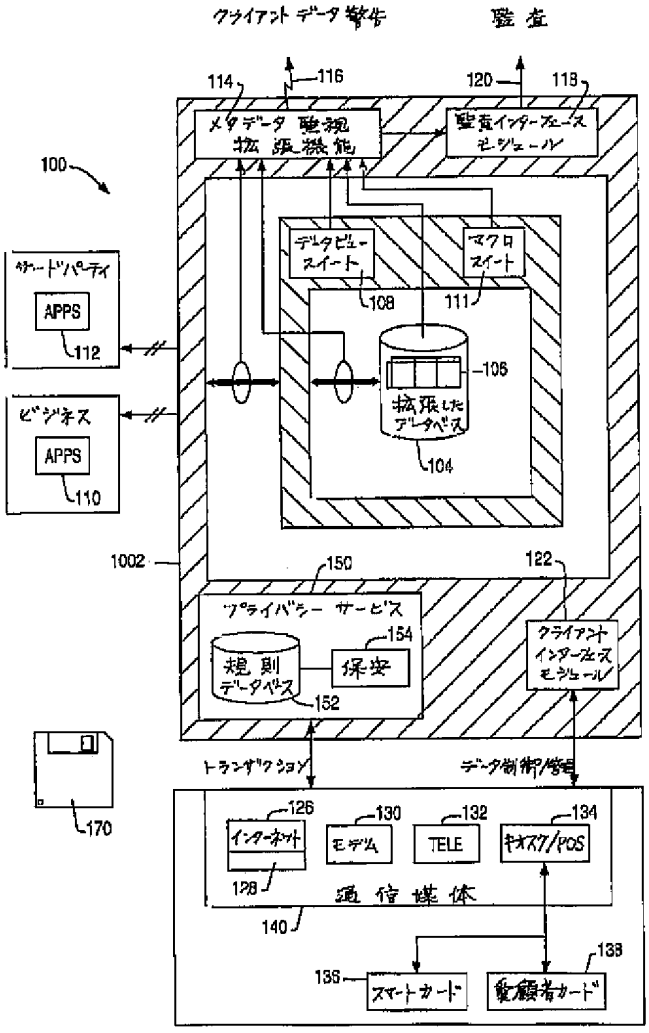
【図8】


エンター
802
データソースからアクセスリクエストを受信する
804
クライアントに特権データビューを与える。
特権データビューはデータソースの個人プライバシーパラメータへのアクセスを与え、データソースの個人プライバシーパラメータの変更を許可する。
リターン

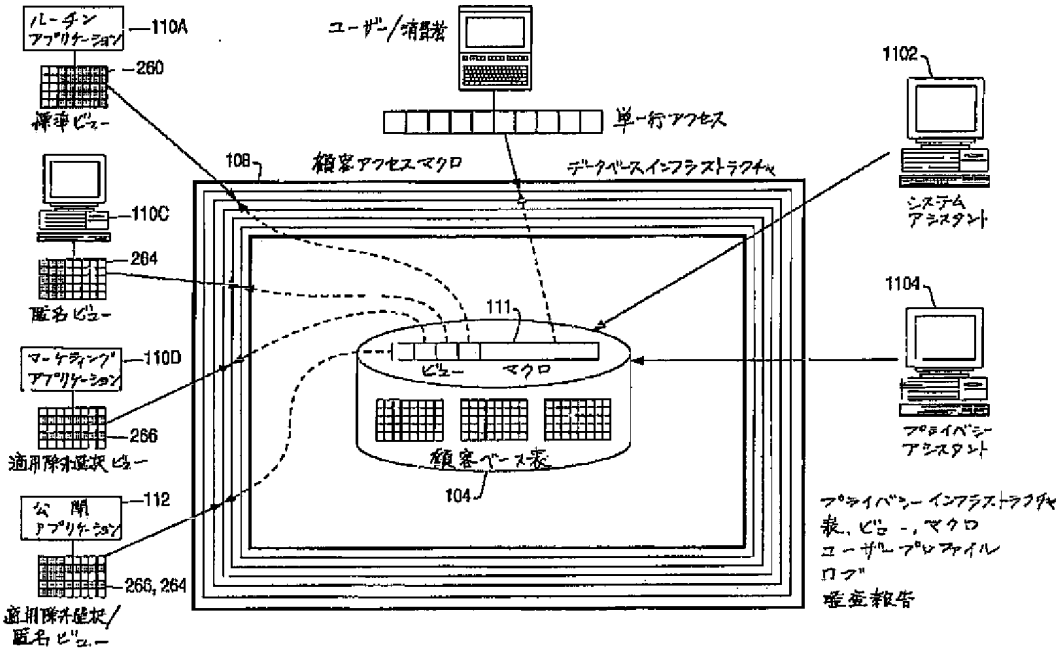
【図9】


監査
クライアント
データ 警告
100
102
120
116
監査
インターフェース
モジュール
118
メタデータ 監視
拡張機能
114
サードパーティ
APPS
112
109
910
904
信託
データベース
902
110
(署名と特元データ)
ビジネス
APPS
110
匿名
保護
インターフェース
モジュール
160
クライアント
インターフェース
モジュール
122
プライバシー サービス
規則
データベース
152
保安
154
150
908
匿名化した
データベース
906
(署名とデータ)
トランザクション
データ制御/管理
126
130
132
134
インターネット
モデム
IELE
キオスク/POS
128
通信媒体
140
136
スマートカード
受領者カード
138
クライアント

【図10】


クライアント データ 警告
監査
114
116
120
118
メタデータ 監視 拡張機能
監査インターフェース モジュール
100
データビュー スイート
マクロ スイート
108
111
APPS
112
106
拡張した データベース
104
ビジネス
APPS
110
1002
150
122
プライバシー サービス
154
規則 データベース
保安
152
クライアント インターフェース モジュール
170
トランザクション
データ制御/管理
126
130
132
134
インターネット
モデム
TELE
キオスク/POS
128
通信媒体
140
138
136
スマートカード
顧客者カード

【図11】



フロントページの続き

(72)発明者 ケネス ダブリュー オフラハティー
アメリカ合衆国 92130 カリフォルニア州 サン ディエゴ トリー ビュー コート 3765

(72)発明者 リチャード ジー ステルワゴン ジュニア
アメリカ合衆国 92064 カリフォルニア州 ポーウェイ カミノ デル バーレ 13035

(72)発明者 トッド エー ウォルター
アメリカ合衆国 92064 カリフォルニア州 ポーウェイ ストートウッド ストリート 12600

(72)発明者 レイド エム ワッツ
アメリカ合衆国 29072 サウスキャロライナ州 レキシントン スプリング クリーク コート 201

(72)発明者 デビッド アレン ラムゼイ
アメリカ合衆国 29072 サウスキャロライナ州 レキシントン ベレ チェイス ドライブ 124

(72)発明者 アドリアン ダブリュー ベルドフイセン
アメリカ合衆国 92069 カリフォルニア州 サン マルコス ターンベリー ドライブ 1661

(72)発明者 レンダ ケー オズデン
アメリカ合衆国 92128 カリフォルニア州 サン ディエゴ キャンドリッジ ロード 12019

(72)発明者 パトラリック ビー デンプスター
アメリカ合衆国 07716 ニュージャージー州 アトランティック ハイランズ ペープ ドライブ 59